M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
Brandon P. Jack (SBN 325584)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
6200 Canoga Avenue, Suite 375
Woodland Hills, CA 91367
Tel: (747) 777-7748
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Attorneys for Plaintiff and the Proposed Class
[Additional counsel on signature page]

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

BRENDEN SMITH; individually and on behalf of all others similarly situated, Plaintiff, v. ENTERTAINMENT PARTNERS, LLC, a Delaware Limited Liability Company, Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

I. INTRODUCTION

1. Plaintiff Brenden Smith ("Plaintiff") brings this class action in this Court under 28 U.S.C. § 1332(d) against Defendant Entertainment Partners, LLC ("Defendant"), for its failure to properly secure and protect Plaintiff's and Class members' personally identifiable information ("PII") from foreseeable cyber threats,[1] resulting in the theft and dissemination of their PII on the dark web (the "Data Breach"). The PII that was stolen in the Data Breach included (but was not necessarily limited to) Plaintiff's and Class members' names, mailing addresses, Social Security numbers, and tax identification numbers.

2. Defendant offers production companies cloud-based related to production finance and production management.[2] Defendant states that it provides "integrated, cloud-based digital solutions supporting every phase of production" with its Smart Accounting tool, Central Casting background actor database, and other production finance and management services.[3]

3. According to Defendant's website, Defendant processes payroll for the entertainment industry, handling compensation for "420K+ production employees" and writing "9.6M+" paychecks annually in North America.[4]

4. As a regular and necessary part of its business, Defendant collects, maintains, and stores sensitive and non-public data pertaining to the personnel working on the productions it services. In this way, Defendant obtained, digitized, aggregated, and stored the PII of Plaintiff and Class members, including salary and compensation

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] https://www.ep.com/company/about-us/ (last visited August 10, 2023).

[3] *Id.*

[4] https://www.ep.com/payroll/ (last visited August 10, 2023).

information, job history and status, income tax information, and contact and identification information.

5. On or before June 30, 2023, Defendant detected suspicious activity within its computer network. A month after being made aware of the suspicious activity, on July 31, 2023, Defendant finally sent out a letter to Plaintiff and Class members informing them that their PII had been stolen by criminals.

6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class members, Defendant assumed legal and equitable duties to protect and safeguard that information from unauthorized access and intrusion. Without the PII of Plaintiff and Class members, Defendant would have been unable to provide its payroll and other services.

7. The stolen PII of Plaintiff and Class members has already been sold or offered for sale on the dark web to identity thieves and used to commit fraud and other crimes that inflict harm on Plaintiff and Class members. Hackers target companies like Defendant to access and then offer for sale the PII to other criminals. In this case, Creditwise searched and located Plaintiff's name, mailing address, and Social Security number on the dark web on August 9, 2023. Plaintiff and Class members now face an ongoing and lifetime risk of identity theft, which is heightened here by the theft of their Social Security numbers in conjunction with verifying information like the names and mailing addresses of Plaintiff and Class members.

8. The PII was targeted and stolen because of Defendant's negligent acts and omissions regarding its data security practices. Defendant failed to take reasonable measures to monitor weaknesses in its data security, failed to timely update, patch, and correct vulnerabilities, and failed to detect and prevent the Data Breach that resulted in criminals stealing Plaintiff's and Class members' PII. In addition, Defendant waited an entire month after the Data Breach occurred to notify affected individuals, which prevented them from timely mitigating the consequences of the Data Breach.

9. As a result of this delayed notification, Plaintiff and Class members had no idea that their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. Because of the sensitive and immutable nature of the PII stolen, this risk will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to adequately protect the PII and to provide timely notification of the Data Breach.

11. Plaintiff and Class members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their PII, and (v) the present, continued, and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

12. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class members was safeguarded, failing to take reasonable steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols concerning data security and failing to enact policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class members was stolen by criminals. Plaintiff and Class members have a continuing interest in ensuring that

their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Brenden Smith is a citizen of Pataskala, Ohio.

14. Defendant is a Delaware limited liability company with its headquarters, membership, and management located in California, at the principal address 2950 North Hollywood Way, Burbank, CA 91505.

III. JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class member is a citizen of a state different from Defendant.

16. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered and operates in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

17. Plaintiff and Class members are past and current employees or contractors who worked on or were otherwise compensated in connection with productions for which Defendant provided payroll or other cloud-based production management services.

18. Plaintiff and Class members provided and entrusted Defendant with sensitive and confidential information, including their names, mailing addresses, Social Security numbers, and tax identification numbers. Defendant required that it be

entrusted with this PII as a condition of providing its services and/or employment. Plaintiff and Class members had essentially no choice by to provide their PII to Defendant to work on the productions.

19. Defendant used Plaintiff's and Class members' PII to derive a substantial portion of its revenue. Without the PII of Plaintiff and Class members, Defendant would have been unable to provide services to the production companies that paid Plaintiff and Class members.

20. Plaintiff and Class members value the security of their PII and expect reasonable security to safeguard their PII. Plaintiff and Class members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information only in connection with providing them payroll services, and to make only authorized and appropriate disclosures of this information.

21. As a result of collecting and storing the PII of Plaintiff and Class members for its own pecuniary benefit, Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class members from improper disclosure to third parties, including foreseeable and preventable data breaches.

The Data Breach

22. On July 31, 2023, Defendant mailed Plaintiff and Class members a letter, which upon opening, stated *Notice of Security Breach* (the "Letter").[5] The envelope did not indicate the importance of the message. In the Letter, Defendant's President and CEO, Markham L. Goldstein, says, "I am writing to let you know that Entertainment Partners experienced a security incident that resulted in unauthorized access to a subset of our accounting application data that included your personal information."[6]

[5] See attached hereto as **Exhibit A** the *Notice of Security Breach* dated July 31, 2023 addressed to Plaintiff Brenden Smith.

[6] *Id.*

23. The letter is sparse on details, explaining only that:

> **What Happened**? On the morning (Pacific Time) of Friday, June 30, 2023, we detected suspicious activity within a limited area of our computer network that supports a subset of our accounting applications. We promptly took the applications offline, notified law enforcement, and engaged industry leading cybersecurity experts to investigate. Over the course of the following few weeks, we determined that a sophisticated threat actor evaded our cybersecurity defenses and acquired database files containing your personal information.
>
> **What Are We Doing**? We are continuing to work with federal law enforcement and our cybersecurity experts. We have restored the applications. We will continue to prioritize additional investments in our cybersecurity defenses. We will continue to monitor online forums and marketplaces for any information relating to this event; we have found none to date.
>
> **What Information Was Involved**? The database files included your name, mailing address, social security number and/or tax identification number in connection with prior productions on which you worked. Please note that your compensation information was not affected.[7]

24. Defendant's letter also stated that it "continue[s] to prioritize additional investments in [its] cybersecurity defenses."[8] However, the details of those investments

[7] *Id.*

[8] *Id.*

have not been shared with Plaintiff and Class members, who retain a vested interest in ensuring that their information remains protected.

25. Defendant has not shared many details regarding the cause of the Data Breach and its impact. However, the fact that "threat actors" extracted entire database files containing PII and the Letter's omission regarding whether the PII was encrypted, implies that the PII was stored in the database unencrypted, or insufficiently encrypted. Data breach notification letters typically include the fact that the PII was encrypted if indeed it was.

26. Plaintiff's and Class members' unencrypted PII, which was acquired by "sophisticated threat actors," already has or will likely end up for sale on the dark web, or into the hands of companies that will use the PII for targeted marketing without the approval of Plaintiff and Class members. As a result of the Data Breach, unauthorized individuals can easily access the PII of Plaintiff and Class members.

27. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted PII it was collecting, digitizing, and aggregating, and insecurely storing in its business, causing the theft of PII by "sophisticated threat actors." Specifically, Defendant failed to exercise reasonable care by: failing to encrypt the PII in storage, retaining PII long after its legitimate purpose for maintaining the PII ended; failing to regularly update passwords; failing to adequately train employees in best practices relating to data security, such as recognizing phishing attempts; failing to erect firewalls and to otherwise segment its network so that Plaintiff's and Class members' PII was not accessible from public-facing computer environments; and failing to use software and personnel that can adequately detect network vulnerabilities, keep current on patches of known vulnerabilities, and monitor network activity to put a stop to the Data Breach before the criminals gained access to and executed commands on Defendant's systems to copy or impound and extract the PII stored in Defendant's databases.

28. Defendant further exacerbated the impact of the Data Breach by keeping news of the Data Breach a secret from Plaintiff and Class members between June—when it was alerted to the suspicious activity—and August—when the Letters finally reached Plaintiff and Class members by mail.

29. Defendant stated that, as soon as it detected suspicious activity, it "notified law enforcement." Defendant could have and should have simultaneously notified Plaintiff and Class members too, and its failure to promptly warn Plaintiff and Class members—whose PII is at stake—was unreasonable and in violation of the law.

Defendant Disregarded and Failed to Account for Known Risks

30. In connection with touting the benefits and quality of its services, Defendant makes buzzword-laden representations regarding its supposed superior data security practices, all of which are intended to induce production companies and Plaintiff and Class members to entrust Defendant with their sensitive PII.

31. For example, Defendant, on its website, states: "At EP, our strategy is 'security first' and employ [sic] an extensive layered security model to protect customer data. Using enterprise policies, people, and technologies, we operate a global security program for end to end protections. From the perimeter to the endpoint, EP's protections and teams work hard to guard the systems that deliver secure products and services to the client."[9]

32. Defendant's represented security features also include: "EP's network security architecture employs modern best practices to segregate environments and data based on risk. This includes the use of separate security zones, comprehensive network segmentation, physically segmented hardware (where necessary), and network access

[9] https://www.ep.com/legal/security-features/ (last visited August 10, 2023)

controls aligned to role-based access. Depending on the zone, enhanced security monitoring and access controls will apply."[10]

33. Contrary to these representations, Defendant failed to reasonably and adequately segment or isolate its network or to erect barriers between accessible points and the stored PII of Plaintiff and Class members. As a result, criminals penetrated Defendant's network by exploiting familiar vulnerabilities and navigated through Defendant's network undetected and unimpeded for as long as it took to acquire Plaintiff's and Class members' PII.

34. Defendant also had this to say: "Encryption at Rest: For sensitive data at rest, EP has deployed an advanced encryption solution with military grade capabilities by enabling policy-based AES-256 encryption with strong key management standards to address modern threats."[11]

35. Contrary to these representations, the files containing Plaintiff's and Class members' PII (undoubtedly sensitive data) that were stolen by criminals in the Data Breach were not encrypted at all or were insufficiently encrypted.

36. Because Defendant had a duty to protect Plaintiff's and Class members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

37. As evidenced by Defendant's statements regarding data security, Defendant knew or should have known that (i) cybercriminals were targeting companies that deal with large quantities of sensitive PII such as Defendant, (ii) its data security practices were deficient, out-dated, and did not comport with its representations, and (iii) cybercriminals were publishing stolen PII on the dark web or using it for other nefarious purposes.

---

[10] *Id.*

[11] *Id.*

38. In light of information readily available and accessible on the Internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiff and Class members in an Internet-accessible environment, had reason to be on guard for the exfiltration of PII and knew that due to its public profile, Defendant had cause to be particularly on guard against such an attack.

39. Prior to the Data Breach, Defendant knew and understood the foreseeable risk that Plaintiff's and Class members' PII could be targeted, accessed, exfiltrated, and published as the result of a cyberattack.

40. Prior to the Data Breach, Defendant knew or should have known that encryption of the PII was required.

41. Prior to the Data Breach, Defendant knew or should have known that it had to delete and destroy PII that it no longer needed to perform its services.

42. Prior to the Data Breach, Defendant knew or should have known that it should not store sensitive and confidential information in an Internet-accessible environment without necessary encryption, detection, and other basic data security precautions that would have prevented this Data Breach.

43. Defendant's negligence in safeguarding the PII of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

44. In light of recent high profile data breaches at other companies providing professional financial services and cloud-based data solutions, Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

45. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

///

///

Securing PII and Preventing Data Breaches

46. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class members from being stolen by criminals.

47. Defendant could have prevented the Data Breach by taking reasonable data security measures, including properly securing and encrypting the folders, files, and/or data fields containing the PII of Plaintiff and Class members. In addition, Defendant should have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so and with proper safeguards. Defendant also should have adequately isolated the sensitive PII from externally accessible points within its network. Defendant should have implemented adequate network monitoring tools and practices to thwart and mitigate attempts to infiltrate its network or the exfiltration of sensitive data, like Plaintiff's and Class members' PII.

48. Several best practices have been identified that, at a minimum, should be implemented by Defendant but were not, including but not limited to: properly training its employees to recognize phishing and other social engineering techniques; employing strong passwords; regularly updating passwords; implementing multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; and limiting access to sensitive data.

49. Other best cybersecurity practices that Defendant should have but did not employ, include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; protecting against any possible communication

system; training staff regarding critical points; and increasing the frequency of penetration testing.

50. These foregoing measures and practices represent applicable and reasonable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

Defendant Violated the Federal Trade Commission Act

51. Federal and State governments have likewise established security standards and issued recommendations to prevent and limit the impact of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[12]

52. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[13] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

53. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[14]

54. The FTC recommends that businesses:

---

[12] Federal Trade Commission, *Start With Security*, *available at*: https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited August 10, 2023)

[13] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited August 10, 2023)

[14] FTC, *Start With Security*, *supra* note 8.

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an Internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the Internet.

g. Determine whether a border firewall should be installed where the business's network connects to the Internet. A border firewall separates the network from the Internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the

network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

55. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

56. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

57. Defendant was at all times fully aware of its obligation to protect the personal and financial data of Plaintiff and Class members. Defendant was also aware of the significant repercussions when it failed to do so.

58. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class members' PII—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Plaintiff and Class Members Face a Substantial Risk of Imminent Harm

60. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

61. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

62. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials and financial account information, or trick victims into paying them their money. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

---

[15] 17 C.F.R. § 248.201 (2013).

[16] *Id.*

63. The Social Security Administration explains that:

> Identity theft is one of the fastest growing crimes in America. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited August 10, 2023).

64. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

65. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[18] Victims of the

[17] *Data Breaches Are Frequent*, *supra,* page 29.

[18] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RESOURCE CENTER (2021),

Data Breach, like Plaintiff and Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[19]

66. According to the Attorney General of California, "Getting a new social security number is probably not a good idea."

> Victims of identity theft sometimes want to change their Social Security number. The Social Security Administration very rarely allows this. In fact, there are drawbacks to changing your number. It could result in losing your credit history, your academic records, and your professional degrees. The absence of any credit history under the new SSN would make it difficult for you to get credit, rent an apartment, or open a bank account.[20]

67. As a direct and proximate result of the Data Breach, Plaintiff and Class members have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiff and Class members must now expend considerable time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

---

https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited August 10, 2023).

[19] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013) http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf (last visited August 10, 2023).

[20] https://oag.ca.gov/idtheft/facts/your-ssn (last visited August 10, 2023).

68. As a result of the Data Breach, Plaintiff's PII is on the dark web. Creditwise scans the dark web daily for consumer personal information. Plaintiff opened an account with Creditwise after learning of the Data Breach. On August 9, 2023, Creditwise found Plaintiff's SSN compromised on the dark web associated with his name and mailing address—the same pieces of information Defendant failed to protect in the Data Breach.

69. Plaintiff and Class members have suffered, and will continue to suffer, actual harms for which they are entitled to compensation, including for:

a. Trespass, damage to, and theft of their personal property including PII;

b. Improper disclosure of their PII;

c. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their PII used against them by spammers and phishers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of their PII for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

70. Moreover, Plaintiff and Class members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. To the extent that Defendant's legitimate business interests no longer warrant retaining their PII, copies of the PII should be destroyed.

71. The injuries to Plaintiff and Class members were, and will continue to be, directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class members.

Value of Personal Identifiable Information

72. The PII of individuals is of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.

73. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not by a price at which consumers themselves actually seek to sell it, but rather in the economic benefit consumers derive from being able to use it and control the use of it. For example, Plaintiff and Class members were only able to obtain services from Defendant after providing their PII. A consumer's ability to use their PII, and businesses' ability to rely on the integrity of that information, is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

74. Plaintiff's and Class members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be

used in a variety of sordid ways for criminals to exploit Plaintiff and Class members and to profit off their misfortune.

75. The information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

76. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against a company like Defendant is to get information to leverage in order to obtain money.

77. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[21] For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

Application of California Law to the Claims of Plaintiff and Class Members

79. California has a significant interest in regulating the conduct of businesses operating within its borders. California seeks to protect the rights and interests of all California residents and citizens of the United States against a company with its principal place of business in California. California has a greater interest in the claims of Plaintiff and Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

80. The principal place of business of Defendant, located in Burbank, California, is the "nerve center" of its business activities – the place where its high-level

[21] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, July 5, 2007, https://www.gao.gov/assets/gao-07-737.pdf (last visited August 10, 2023)

officers direct, control, and coordinate the company's activities, including its data security functions and policy, financial, and legal decisions.

81. Defendant's response to the Data Breach, and corporate decisions surrounding such response, were made from and in California.

82. Defendant's breaches of duty to Plaintiff and Class members emanated from California.

83. Application of California law to the Class with respect to Plaintiff's and Class members' claims is neither arbitrary nor fundamentally unfair because California has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and Class members.

84. Under California's choice of law principles, the common law of California applies to the common law claims of all Class members. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, California's Unfair Competition Law may be applied to non-resident consumer Plaintiff as against this resident-defendant. Further, Defendant's General Terms and Conditions include a venue provision (Section 9.2) selecting venue within Los Angeles County, California, as well as a choice-of-law provision (Section 9.2) selecting the laws of the State of California, without giving effect to conflict of laws provisions.[22]

V. CLASS ALLEGATIONS

78. Plaintiff brings this nationwide class action on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

79. The Class that Plaintiff seeks to represent is defined as follows:

[22] https://www.ep.com/legal/terms-and-conditions/ (last visited August 10, 2023)

> All individuals whose PII was compromised in the data breach that is the subject of the *Notice of Security Breach* that was sent to Plaintiff and Class members on or around July 31, 2023.

80. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

81. Plaintiff reserves the right to modify or amend the definition of the proposed classes as appropriate.

82. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Defendant has identified numerous individuals whose PII was compromised in the Data Breach, and the Class members are apparently identifiable within Defendant's records.

83. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact are common to the Class members and predominate over any questions affecting only individual Class members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class members;

b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiff and Class members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PII had been stolen;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class members;

k. Whether Plaintiff and Class members are entitled to actual, statutory, liquidated, nominal, consequential, and/or punitive damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class members are entitled to injunctive relief.

84. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class members because they all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

85. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

86. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class members in that they have no conflicts of interest with other Class members. Plaintiff seeks no relief that is antagonistic or adverse to the Class members and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

87. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

88. The nature of this action and the nature of laws available to Plaintiff and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

89. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

90. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

91. Unless a class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class members, Defendant may continue to refuse to provide proper notification to Class members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this complaint.

92. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

93. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution

of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class members; and,

i. Whether Class members are entitled to damages and equitable relief, including restitution and injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence

94. Plaintiff re-alleges paragraphs 1-93 as if fully set forth herein.

95. Plaintiff and Class members provided and entrusted, or otherwise authorized Defendant to collect their PII with the understanding that Defendant would take reasonable and appropriate steps to safeguard the PII, use the PII for legitimate business purposes only, and not disclose their PII to unauthorized third parties.

96. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class members would suffer if the PII were wrongfully disclosed.

97. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and Class members involved an unreasonable risk of harm to Plaintiff and Class members, due to the significant and foreseeable risk of harm through the criminal acts of third parties.

98. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting Plaintiff's and Class members' PII from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and Class members in Defendant's possession was adequately secured and protected.

99. Defendant also had a duty to exercise appropriate practices to destroy PII it was no longer required to retain pursuant to regulations and had no reasonable need to maintain.

100. Defendant also had a duty to put procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and Class members.

///

///

101. Defendant also had a duty to protect against the reasonably foreseeable criminal conduct of a third party as it was on notice that the failure to protect the PII that it collected for its own benefit would result in harm to Plaintiff and Class members.

102. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class members. That special relationship arose because Plaintiff and Class members entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant, based on Defendant's assurances that the information would be protected by superior data security practices.

103. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and Class members.

104. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

105. Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Plaintiff's and Class members' PII, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

106. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class members' PII, including basic encryption techniques freely available to Defendant.

107. Plaintiff and Class members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

108. Defendant was in an exclusive position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach.

109. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of Plaintiff's and Class members' PII.

110. Defendant has admitted that Plaintiff's and Class members' PII was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

111. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class members by failing to implement proper data protection protocols in accordance with industry standards and failed to exercise reasonable care in protecting and safeguarding Plaintiff's and Class members' PII.

112. Defendant improperly and inadequately safeguarded Plaintiff's and Class members' PII in violation of standard industry rules, regulations, and practices at the time of the Data Breach.

113. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect Plaintiff's and Class members' PII in the face of increased risk of theft.

114. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect suspicious activity on its network and prevent dissemination of the PII.

115. Defendant breached its duty to exercise appropriate practices by failing to remove from the Internet-accessible environment any PII it was no longer required to retain pursuant to regulations and which Defendant had no reasonable need to maintain.

116. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class members the existence and scope of the Data Breach.

117. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, Plaintiff's and Class members' PII would not have been compromised, stolen, and accessible to wrongdoers on the dark web.

118. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class members' PII and the harm, or risk of imminent harm, suffered by Plaintiff and Class members. Plaintiff's and Class members' PII was stolen as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

119. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of Plaintiff's and Class members' PII.

120. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or

harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

121. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its possession.

COUNT II
Breach of Implied Contract

122. Plaintiff re-alleges paragraphs 1-93 as if fully set forth herein.

123. Defendant required Plaintiff and Class members to provide their PII in order for them to obtain employment and/or Defendant's services.

124. Defendant's Privacy Policy, advertising and marketing materials, and website representations made enforceable promises that Plaintiff's and Class members' PII would be kept secure and confidential, would be used only for legitimate purposes to serve Plaintiff and Class members, and would not be disclosed to unauthorized third parties.

125. Defendant promised to "use commercially reasonable technical, organizational, and administrative measure to protect its websites, online services, payroll services and casting services against unauthorized or unlawful access and against accidental loss, theft, disclosure, copying, modification, and destruction, or damage.[23]

126. Defendant promised to retain Plaintiff's and Class members' information only for as long as their account is active, for as long as needed to provide services requested, or as long as needed to comply with legal obligations.

[23] https://www.ep.com/legal/privacy-notice/ (last visited August 10, 2023).

127. Plaintiff and Class Members only provided their PII because there was an implicit agreement that Defendant would secure and protect their PII from disclosure to any unauthorized third party, and to timely and accurately notify Plaintiff and Class members in the event of a Data Breach.

128. Plaintiff and Class members would not have provided their PII to Defendant had they known that Defendant would fail to perform its promises to safeguard and protect their PII and provide accurate and timely notice of the Data Breach.

129. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendant.

130. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' PII and by failing to provide them with timely and accurate notice of the Data Breach. More specifically, Defendant breached the implied contracts it made with Plaintiff and Class members by (i) failing to use commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of Plaintiff's and Class members' PII, (ii) failing to encrypt the PII in storage, (iii) failing to delete PII it no longer had a reasonable need to maintain, and (iv) otherwise failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

131. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class members have suffered and will continue to suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data

Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' PII; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of Plaintiff's and Class members' PII.

132. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class members are entitled to recover actual, consequential, and nominal damages.

COUNT III
Violations of California's Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*.

133. Plaintiff realleges paragraphs 1–93 as if fully set forth herein.

134. The UCL prohibits any "unlawful" or "unfair" business act or practice, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful and unfair practices within the meaning, and in violation, of the UCL.

135. In the course of conducting its business, Defendant committed "unlawful" business practices by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII, and by violating the statutory and common law alleged herein, including, inter alia, Article I, Section 1 of the California Constitution (California's constitutional right to privacy), Cal. Civil Code § 1798.81.5,

45 C.F.R. § 164, *et seq.*, and the FTC Act. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, and want of ordinary care are ongoing and continue to this date.

136. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

137. Defendant violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein and storing Plaintiff's and Class members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class members. The harm these practices caused to Plaintiff and Class members outweighed their utility.

138. Defendant's above-described wrongful actions, inaction, want of ordinary care, and practices also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA and the FTC Act. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

139. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of statutory and common law. Plaintiff and the Class members suffered from overpaying for services that should have included adequate data security for their PII, by experiencing a diminution of value and loss of the control over who uses their PII as a result if its theft by cybercriminals, the loss of Plaintiff's and Class members' legally protected interest in the confidentiality and privacy of their PII, and additional losses as described above.

140. Plaintiff and Class members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII for which there is a well-established national and international market, and/or (v) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

141. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. As such, Plaintiff and Class members, seek restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Cal. Bus. & Prof. Code § 17203. To the extent any of these remedies are equitable, Plaintiff and Class members seek them in the alternative to any adequate remedy at law they may have.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and Plaintiff's counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal

security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

///

///

D. For an award of damages, including actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: August 10, 2023

Respectfully Submitted,

M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
Brandon P. Jack (SBN 325584)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
6200 Canoga Avenue, Suite 375
Woodland Hills, CA 91367
Tel: (747) 777-7748
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Marc E. Dann*
Brian D. Flick*
DANNLAW
15000 Madison Avenue
Lakewood, OH 44107
Tel: (216) 373-0539
Fax: (216) 373-0536
mdann@dannlaw.com
notices@dannlaw.com

Thomas A. Zimmerman, Jr.*
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Tel: (312) 440-0020
tom@attorneyzim.com
sharon@attorneyzim.com
firm@attorneyzim.com

**pro hac vice* forthcoming

Attorneys for Plaintiff and the Proposed Nationwide Class and Subclasses